Ei des Kolumbus – oder Kuckucksei?

Microsoft Office 365 und Datenschutz

Christoph Schäfer
Secorvo Security Consulting GmbH

Als Christoph Kolumbus 1493 von seiner ersten Reise nach Amerika zurückgekehrt war, soll er zu einem Festmahl mit bei Kardinal Mendoza eingeladen worden sein. Auf den Bericht seiner Reise hin, hielt man ihm entgegen, dass seine Entdeckung nicht außergewöhnlich gewesen sei – jeder andere hätte das auch gekonnt. Daraufhin soll Kolumbus die anwesenden Zweifler gebeten haben, ein hartgekochtes Ei auf eine der Spitzen zu stellen. Niemandem gelang es. Kolumbus schlug das Ei mit der Spitze auf den Tisch und stellte es hin. Empört wurde ihm vorgehalten, jeder hätte das tun können. Kolumbus erwiderte: „Der Unterschied ist, meine Herren, dass Sie es hätten tun können, ich hingegen habe es getan."

Das Ei des Kolumbus

IT-Outsourcing in "die Cloud" liegt im Trend. Die Anbieter locken mit skalierbaren und anpassungsfähigen Anwendungen und Infrastrukturen. Bei Cloud-Dienstleistungen befinden sich Hard- und Software ganz oder teilweise in den Rechenzentren des Anbieters. Auch kurzfristige Anpassungen an den tatsächlichen Bedarf sind oft viel schneller möglich als beim klassischen Outsourcing. Höhere Flexibilität bei geringeren Kosten ist die gewünschte Folge.

Eine solche Lösung ist auch Microsoft Office 365, bei dem die Anwendung aus der Microsoft-Cloud bezogen und Dokumente und E-Mails in Microsoft-Rechenzentren gespeichert werden. Könnte das das moderne Ei des Kolumbus sein?

Immer dieser Datenschutz

Während Cloud-Anwendungen bei Nutzern und IT-Verantwortlichen oft Jubelschreie ob der Möglichkeiten auslösen, zucken Datenschützer eher zusammen. Gerade wenn es um außereuropäische Anbieter geht, sind viele rechtliche Vorgaben zu beachten.

Oft überrascht der Ansatz des Gesetzgebers: Grundsätzlich darf man keine personenbezogenen Daten erheben, verarbeiten oder nutzen. Von dieser Regel gibt es zwei Ausnahmen: Entweder ein Gesetz erlaubt es bzw. ordnet es an oder der Betroffene, dessen Daten verarbeitet werden sollen, hat eingewilligt. Man spricht hierbei vom „Verbot mit Erlaubnisvorbehalt".[1]

Das Erheben, Verarbeiten und Nutzen sowie die Übermittlung personenbezogener Daten für eigene Geschäftszwecke ist zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines Vertrages mit dem Betroffenen erforderlich ist[2]; es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen des Betroffenen dem entgegenstehen[3] oder wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte[4].

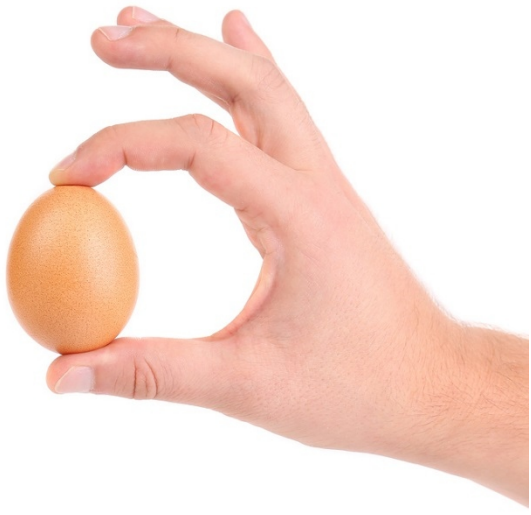


Bild: Indigolotos/Bigstock.com

Eine Form des Verarbeitens im Sinne des

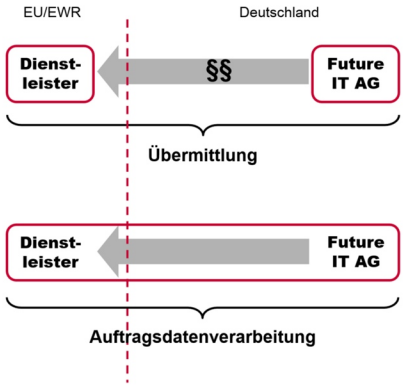
1 § 4 Abs. 1 BDSG
2 § 28 Abs. 1 Satz 1 Nr. 1 BDSG
3 § 28 Abs. 1 Satz 1 Nr. 2 BDSG
4 § 28 Abs. 1 Satz 1 Nr. 3 BDSG

Datenschutzes ist das Übermitteln[5] personenbezogener Daten. Dies liegt immer dann vor, wenn gespeicherte oder durch Datenverarbeitung gewonnene personenbezogene Daten Dritten[6] (außerhalb der für die Datenverarbeitung verantwortlichen Stelle) durch Weitergabe oder durch Bereithalten zum Abruf oder zur Einsicht bekanntgegeben werden.

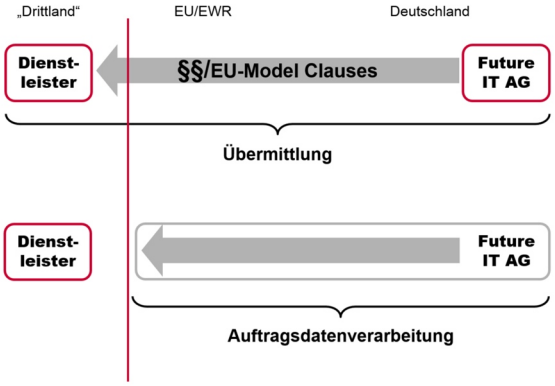
Für eine solche Übermittlung bedarf es einer Rechtsgrundlage, die unter Umständen nicht ohne größeren Aufwand oder auch gar nicht nachgewiesen werden kann.

Datenschutz und Dienstleister

Als Dritte gelten jedoch nicht Personen oder Stellen, die im Inland, in einem anderen Mitgliedstaat der EU/EWR personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen (Auftragsdatenverarbeitung[7]).[8] Liegen die Voraussetzungen vor und schließt man einen entsprechenden Vertrag mit dem Dienstleister, erspart man sich das Erfordernis einer gesonderten Rechtgrundlage. Dies macht viele Datenverarbeitungen durch Dienstleister überhaupt erst möglich, da man hierdurch nicht z. B. Einwilligungen aller seine Kunden einholen muss.



Problematischer wird es, wenn der Dienstleister in einem sogenannten Drittland (außerhalb EU/EWR) sitzt. Eine Auftragsdatenverarbeitung ist in diesem Fall gar nicht möglich, so dass nur die Übermittlung als Lösung bleibt. Das Bundesdatenschutzgesetz (BDSG) stellt besondere Anforderungen an die Zulässigkeit einer Übermittlung in Drittländer.



Die Übermittlung ist unzulässig, wenn der Betroffene ein sogenanntes schutzwürdiges Interesse an dem Ausschluss hat, insbesondere dann, wenn bei den empfangenden Stellen außerhalb der EU kein angemessenes Datenschutzniveau gewährleistet ist. Die Gewährleistung eines angemessenen Datenschutzniveaus kann unter anderem durch den Abschluss sogenannter EU-Standardvertragsklauseln (EU-Model Clauses) oder derzeit bei Stellen in den USA durch deren Unterwerfung unter das Safe Harbor Abkommen erfolgen. Den Datenschutz-Aufsichtsbehörden genügt Safe Harbor allerdings nicht aus – es müssen weitere Nachweise über das Schutzniveau erbracht werden (bspw. Zertifizierungen).

Besondere Daten, besondere Probleme

Während man für „normale" personenbezogene Daten noch relativ schnell eine datenschutzrechtliche Lösung finden kann, gibt es bestimmte Daten und Regelungen, die zusätzlich beachtet werden müssen.

Bei sogenannten besonderen Arten personenbezogener Daten (Angaben über die rassische/ethnische Herkunft, politische Meinung, religiöse/philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) gelten zusätzliche Anforderungen – die schutzwürdigen Interessen der Betroffenen sind besonders

5 § 3 Abs. 4 Satz 2 Nr. 3 BDSG
6 § 3 Abs. 8 Satz 2 BDSG
7 § 11 BDSG
8 § 3 Abs. 8 Satz 3 BDSG

hoch zu gewichten, weswegen eine Interessensabwägung als Rechtsgrundlage für die Übermittlung ausscheidet.

Sind Daten von Berufsgeheimnisträgern (Rechtsanwälte, (Betriebs-)Ärzte, Steuerberater, Psychologen…) betroffen, muss eine unberechtigte Kenntnisnahme der Daten[9] ausgeschlossen sein – auch durch Administratoren.

Will man Steuerdaten außerhalb Deutschlands speichern, bedarf es einer Genehmigung der Finanzbehörden.[10] In Betriebsvereinbarungen sind unter Umständen Ausschlüsse von Cloud-Datenverarbeitungen zu finden. Außerdem können vertragliche Ausschlüsse von Cloud-Verarbeitung mit Kunden vereinbart sein, deren Missachtung zu hohen Vertragsstrafen führen kann.

Während man die letzten Punkte schlicht beachten und ggf. regeln muss, bestehen insbesondere bei der Cloud-Verarbeitung besonderen Arten personenbezogener sowie einem Berufsgeheimnis unterliegender Daten hohe Hürden.

Die einzige Möglichkeit, diese Daten eventuell doch bei einem Cloud-Dienstleister verarbeiten zu dürfen, ist eine angemessene Verschlüsselung, die aber gewissen Anforderungen gerecht werden muss. So muss der Auftraggeber die Ver- und Entschlüsselung sowie die Schlüssel selbst vollständig beherrschen. Dies in einer Cloud-Umgebung zu gewährleisten ist nicht trivial und bei Office 365 derzeit nur mit einer Drittanbieter-Lösung denkbar.

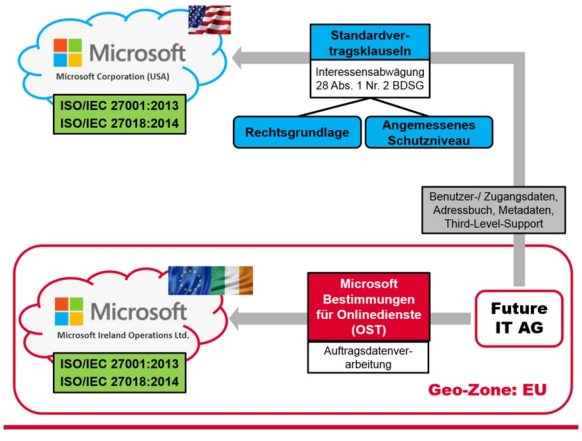
Nadelöhr erkannt

Microsoft hat den Datenschutz schon früh als Nadelöhr erkannt und ist in einen Diskussionsprozess mit den europäischen Aufsichtsbehörden (Art.-29-Gruppe[11]) eingetreten. Das Ergebnis dieses mehrjährigen Prozesses sind die im Juli 2014 veröffentlichten und zuletzt im Januar 2015 aktualisierten Online Service Terms (OST)[12], die eine Vielzahl bisher einzelner Vertragsdokumente zusammenfassen und als Anlage die EU-Standardvertragsklauseln enthalten. Um den europäischen Datenschutzanforderungen gerecht zu werden garantiert Microsoft unter anderem die Speicherung von Daten innerhalb Europas, nämlich in den Rechenzentren in Dublin und Amsterdam.

Ganz ohne die USA kommt Office 365 dennoch nicht aus, da die Microsoft-Infrastruktur auf einen globalen Betrieb ausgerichtet ist. Unter anderem werden das AD-Adressbuch und Metadaten, die teilweise auch personenbezogen sind, auch außerhalb Europas verarbeitet. Hinzu kommen Support-Fälle, in denen die Unterstützung von US-Mitarbeitern erforderlich ist. Daher genügt ein Vertrag zur Auftragsdatenverarbeitung mit Microsoft Irland allein nicht. Zusätzlich müssen die EU-Standardvertragsklauseln mit der Microsoft Corporation (USA) geschlossen werden.

Rechtsgrundlage für Microsoft Office 365

Neben der Vereinbarung zur Auftragsdatenverarbeitung mit Microsoft Irland werden EU-Standardvertragsklauseln mit der Microsoft Corporation (USA) geschlossen. Da dies mit einer Datenübermittlung in die USA einhergeht, wird eine Rechtsgrundlage benötigt. Wie eingangs erläutert, kommen dafür eine gesetzliche Erlaubnis oder die Einwilligung der Betroffenen (Mitarbeiter und/ oder Kunden) in Betracht.



9 § 203 Abs. 1 StGB

10 § 146 Abs. 2a S. 1 AO

11 http://ec.europa.eu/justice/data-protection/article-29/index_de.htm

12 http://www.microsoftvolumelicensing.com/ DocumentSearch.aspx?Mode=3&DocumentTypeId=31

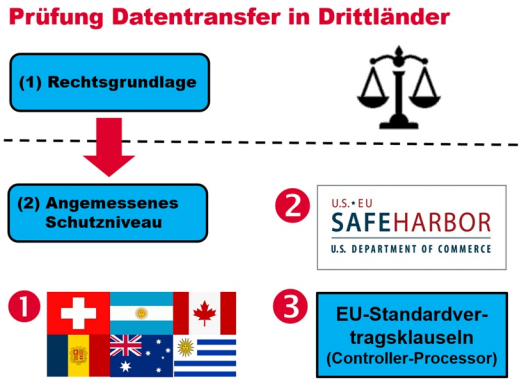
Die Einwilligung der Mitarbeiter scheidet beim Cloud-Outsourcing als Rechtsgrundlage regelmäßig aus, da eine der gesetzlichen Anforderungen an die Einwilligung die Freiwilligkeit[13] derselben ist. Im Arbeitsverhältnis ist Freiwilligkeit kaum zu gewährleisten.

Als gesetzliche Grundlage könnte die Interessensabwägung zwischen den berechtigten Interessen des Unternehmens und den schutzwürdigen Interessen der Mitarbeiter/Kunden herangezogen werden.

Prüfung des Datentransfers in Drittländer

Die Prüfung erfolgt in zwei Schritten:

(1) Es muss eine Rechtsgrundlage gefunden werden.
(2) Im Zielland muss ein angemessenes Datenschutzniveau sichergestellt werden.



Bei der Interessenabwägung als Rechtsgrundlage muss eine sorgfältige Abwägung aller Aspekte – positiver wie negativer – erfolgen. Insbesondere muss bewertet werden, welche Arten von Daten in der Cloud verarbeitet werden sollen und welche nicht. Auch mögliche Zugriffe durch US-Strafverfolgungsbehörden oder Geheimdienste müssen bewertet werden. Die möglichen Vorteile eines Cloud-Outsourcings dürfen dabei nicht vergessen werden – möglicherweise kann durch die Auslagerung sogar ein höheres Sicherheitsniveau erreicht werden. In jedem Fall sollte die Abwägung auf Fakten basieren.

Auf der zweiten Prüfungsstufe muss sichergestellt werden, ob im Zielland (hier: USA) ein dem europäischen Datenschutzrecht entsprechendes „angemessenes Schutzniveau“ herrscht. Neben einer von der EU-Kommission definierten Liste[14] von sicheren Drittländern (❶), auf der die USA nicht zu finden sind, käme das Safe-Harbor-Abkommen[15] (❷) in Frage, nach dem US-Firmen ihre Konformität zum EU-Datenschutz erklären. Nicht erst seit den Snowden-Enthüllungen wird Safe-Harbor allerdings stark kritisiert. Auch die Datenschutz-Aufsichtsbehörden weisen darauf hin, dass Safe Harbor allein keine ausreichende Bestätigung für das angemessene Schutzniveau ist.[16] Microsoft bietet daher im Rahmen seiner OST die EU-Standardvertragsklauseln als Grundlage an. (❸)

Trau, schau, wem

Auch nach der Abstimmung des Microsoft-Vertragswerks mit der Art.-29-Gruppe obliegen dem Auftraggeber umfangreiche Prüfpflichten der Verträge. Problematisch ist insbesondere, dass die Auftragsdatenverarbeitung in Deutschland sehr explizit geregelt ist. Dabei finden sich nicht alle Anforderungspunkte des Bundesdatenschutzgesetzes direkt im Vertrag wieder.

…oder Kuckucksei

Vielleicht ist Office 365 aber auch eher ein Kuckucksei. Das Risiko des möglichen Datenherausgabeanspruchs seitens US-Strafverfolgungsbehörden gegenüber Tochterunternehmen und Niederlassungen US-amerikanischer Unternehmen muss bewertet werden. Dies wird besonders in den Medien oft diskutiert und heftig kritisiert. Microsoft wehrt sich derzeit in einem Rechtsstreit in den USA gegen einen solchen Herausgabeanspruch. Der Ausgang des Prozesses kann derzeit nicht abgesehen werden. Die

13 § 4a Abs. 1 Satz 1 BDSG

14 http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

15 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:DE:PDF

16 https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf, Seite 17.

bloße Unterstellung, die USA hätten jederzeit Zugriff auf Daten amerikanischer Unternehmen in Europa, kann jedoch nicht in einer grundsätzlichen Beurteilung der datenschutzrechtlichen Zulässigkeit die rechtliche Unzulässigkeit bereits vor der tatsächlichen Vornahme einer solchen rechtswidrigen Übermittlung annehmen.

Fraglich ist, wie der ebenfalls oft diskutierte Datenzugriff durch (US-)Geheimdienste zu bewerten ist. Hierzu gibt es keine gesicherte Faktenlage, die bewertet werden kann. Der Geheimdienstzugriff ist daher im Rahmen einer Risikoeinschätzung zu betrachten.

Und nun?

Cloud-Datenverarbeitung wird sich vermutlich nicht aufhalten lassen. Derzeit tun sich die Datenschutz-Aufsichtsbehörden in Deutschland noch sehr schwer damit. Unternehmen können sich nicht allein auf die Microsoft-Verträge verlassen. Soll Office 365 eingeführt werden, muss eine ausführliche Prüfung und Bewertung unter anderem durch den betrieblichen Datenschutzbeauftragen erfolgen. Ein rechtliches Restrisiko lässt sich nicht ausschließen.

Office 365 kann möglich sein

Unter den oben dargestellten Voraussetzungen kann ein datenschutzkonformer Einsatz von Microsoft Office 365 möglich sein, wenn er auch nicht frei von Risiken ist. Trotz valider Prüfung bleibt aufgrund der erforderlichen Interessensabwägung als Teil der Rechtsgrundlage aus § 28 Abs. 1 Nr. 2 BDSG ein Rechtsrisiko bezüglich der Auslegung bestehen. Die zuständige Datenschutz-Aufsichtsbehörde könnte zu einer anderen Wertung gelangen und die Datenverarbeitung in Office 365 untersagen.

Dies kann auch nachträglich beispielsweise durch eine Veränderung des Kenntnisstandes über Datenzugriffe oder -herausgabeverlangen aus Drittstaaten eintreten. Übrigens: Microsoft behält sich die Änderungen an seinen Diensten aufgrund der Änderung rechtlicher Rahmenbedingungen vor, so dass der geprüfte Stand plötzlich ganz anders aussehen kann. Für diesen Fall benötigt man eine Fallback-Strategie, um die Daten aus der Cloud zurückholen zu können.

Die Sicht der Aufsichtsbehörden

Insbesondere müssen die künftigen Aussagen von Datenschutz-Aufsichtsbehörden verfolgt werden. Sowohl der Berliner Beauftragte für Datenschutz und Informationsfreiheit als auch der Hamburgische Beauftrage für Datenschutz und Informationsfreiheit haben im Rahmen des 9. Europäischen Datenschutztages am 28.01.2015 geäußert, die Vorgaben für Datenübermittlungen in die USA kritisch prüfen und gegebenenfalls untersagen zu wollen. Der Berliner Beauftragte erklärte sogar, dass das EU-Datenschutzniveau nur bei Online-Angeboten europäischer Unternehmen gewährleistet werden kann. Selbst wenn US-Firmen in Europa Daten speichern würden, können US-Sicherheitsbehörden darauf zugreifen. Inwiefern diese Aussagen in dieser Generalität haltbar sind, ist zumindest fraglich.

Kolumbus oder Kuckuck?

Ob Microsoft Office 365 nun das Ei des Kolumbus oder das des Kuckucks ist, lässt sich weder pauschal noch final beantworten. Unternehmen müssen den Einsatz in jedem Fall sehr kritisch prüfen und letztlich entscheiden, ob der Einsatz trotz eines Rechtsrisikos gewollt ist. Die Antwort auf diese Frage wird je nach Unternehmen unterschiedlich ausfallen.

Zum Autor: Christoph Schäfer ist Security Consultant bei der Secorvo Security Consulting GmbH, zertifizierter betrieblicher Datenschutzbeauftragter (GDDcert.), Datenschutzauditor (TÜV) und TeleTrusT Information Security Professional (T.I.S.P.). Seine Beratungsschwerpunkte sind datenschutzrechtliche Fragestellungen und technisch-organisatorischer Datenschutz. Zudem hält er regelmäßig Schulungen und Vorträge zu Datenschutzthemen.

E-Mail: christoph.schaefer@secorvo.de